COINCIDENCE-FREE MEDIA KEY BLOCK FOR CONTENT PROTECTION FOR RECORDABLE MEDIA

ABSTRACT OF THE DISCLOSURE

A system for protecting content on recordable media for, e.g., DVD audio disks, flash memory media, or other media includes providing a media key block (MKB) on each media, with each MKB including 25,000 encryptions of a media key by 25,000 or so device keys. Each authorized player in the system has a single device key from among the system device keys with which to decrypt the media key. To avoid a coincidence attack in which a hacker can learn the MKB and associated media key and then guess at a device key without knowing its position in the MKB, the media key is XORed with a number representing each position in the MKB, and only then encrypted with the device key corresponding to that position.